Информация

о наиболее распространенных видах мошенничества в сфере информационно-телекоммуникационных технологий и основных мерах предосторожности

ОСНОВНЫЕ СХЕМЫ МОШЕННИЧЕСТВА:

«ВАША КАРТА ЗАБЛОКИРОВАНА»

Банковская карта — это инструмент для совершения платежей и доступа к наличным средствам на счете не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходят сообщения следующего характера: «Ваша банковская карта заблокирована. Инфо по телефону ...» «операция по карте №….. приостановлены. Подробнее по номеру телефона...». В сообщениях предлагается бесплатно позвонить на определенный номер для получения подробной информации.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Мошенники осуществляют СМС-рассылку на различные номера телефонов и ждут звонка. Когда Вы звоните по указанному телефону, Вам отвечает мошенник, который представляется сотрудником службы безопасности банка и под различными предлогами (разблокировка карты, отмена подозрительных операций по Вашей карте, которых Вы не совершали возврат денежных средств, похищенных с вашей карты мошенниками, сбой обслуживания карты и прочее) пытается выяснить у вас номер карты и пароли доступа, поступающих в СМС оповещениях.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

предупреждаем: никому и ни при каких обстоятельствах не сообщайте реквизиты Вашей карты, ПИН-код, одноразовые пароли доступа, которые приходят на телефон и позволяют войти в мобильном банк, а также цифры, указанные на оборотней стороне Вашей карты (CVC2, CVV2 коды)! Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Относитесь к ПИН-коду как к ключу от сейфа с Вашими средствами! Нельзя хранить ПИН — код рядом с картой и тем более записывать ПИН-код на нее — в этом случае Вы даже не успеете обезопасить свой счет, заблокировав карту после кражи или утери! Единственно правильный номер банка казан на оборотной стороне Вашей карты. Для того чтобы убедитесь, что Вашим деньгам ничего не угрожает достатчн7о позвонить в клиентскую службу поддержки банка или обратиться лично в банк.

Внимание! Ни при каких обстоятельствах не сообщайте свои пароли никому, включая сотрудников Банка, не перезванивайте на номер мобильного телефона, указанный в поступившем СМС-сообщении от Банка, не предоставляйте информацию о реквизитах карты (номер карты, срок ее действия, ПИН — коде, контрольной информации по карте), или об одноразовых паролях, в т.ч. посредством направления ответных СМС — сообщений, а также сотруднику банка, не проводите через банкомат никакие операции по инструкциям, полученным по телефону.

Специалисты банков никогда не запрашивают у клиентов информацию о паролях из СМС, от интернет-банка и серийный код карты, так как им эти сведения и так известны.

«НОВЫЙ ВИД МОШЕННИЧЕСТВА»

Это мошенничество основано на возможности подменять любой номер телефона при звонке с ip-телефонии. Вам могут позвонить с номера вашего близкого и сообщить, что он попал в беду (или, например, задержан полицией) и начать требовать деньги, для решения вопроса. Могут позвонить с телефона вашего банка и представившись сотрудником службы безопасности выманить данные Вашей карты, рассказав например, о взломе вашей карты и попытках несанкционированного списания денежных средств, а потом уже узнать у вас всю нужную информацию.

Пожалуйста запомните, мошенники могут подставить ЛЮБОЙ номер. Если вы видите при входящем звонке номер вашего банка, страховой компании, государственной организации, друга или родственника, это НЕ ОЗНАЧАЕТ, что Вам звонит действительно тот, чей это номер. Будьте осторожны!

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Первое и самое главное правило — прервать разговор и самостоятельно перезвонить на абонентский номер близкого человека. Если телефон отключен, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации. В случае если звонили со стационарного номера телефона банка, для того чтобы убедиться, что Вашим деньгам ничего не угрожает достаточно позвонить в клиентскую службу поддержки банка или обратиться лично в банк.

«УДАЛЕННЫЙ ДОСТУП»

Это когда жертва в телефонном режиме, под руководством мошенников установила приложение и предоставила злоумышленникам удаленный доступ к мобильному устройству, и тем самым дают возможность беспрепятственно завладеть персональной информацией и в последующем похитить деньги со счетов через мобильный банк.

КАК ЭТО ОРГАНИЗОВАНО:

Преступник представляется сотрудником банка и сообщает о выявлении вредоносного программного обеспечения на мобильном устройстве клиента. Сообщает, что для его хранения нужно предоставить доступ к устройству. Жертве необходимо скачать на мобильном телефоне программу удаленного доступа TyeamViewer, Anydesk,